

01.06.99

JP 99/02924

日本国特許庁 EU

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 16 JUL 1999

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1998年 6月 2日

出願番号

Application Number:

平成10年特許願第153066号

出願人

Applicant(s):

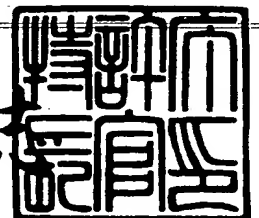
日本電信電話株式会社

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 6月18日

特許庁長官
Commissioner,
Patent Office

山田佐平



出証番号 出証特平11-3043021

【書類名】 特許願

【整理番号】 NTTH105234

【提出日】 平成10年 6月 2日

【あて先】 特許庁長官殿

【国際特許分類】 H04K

【発明の名称】 関数のランダム性評価装置、ランダム関数生成装置、およびそのプログラム記録媒体

【請求項の数】 7

【発明者】

【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

【氏名】 盛合 志帆

【発明者】

【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

【氏名】 青木 和麻呂

【発明者】

【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

【氏名】 神田 雅透

【発明者】

【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

【氏名】 高嶋 洋一

【発明者】

【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

【氏名】 太田 和夫

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 関数のランダム性評価装置、ランダム関数生成装置、およびそのプログラム記録媒体

【特許請求の範囲】

【請求項 1】 評価すべき関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価手段と、

上記評価すべき関数に対し、鍵 k を固定して x を入力して、素数 p 又は p のべき乗個の要素からなるガロア体上の多項式を用いて出力 $y = f_k(x)$ を表現して、上記多項式の項数を求めて補間攻撃法に対する耐性を評価する補間攻撃耐性評価手段と、

上記評価すべき関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関係のその平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と、

評価すべき関数 $S(x)$ について予め決められた Δx に対し $(S(x) + S(x + \Delta x))$ と出力のマスク値 Γy との内積が 1 である x の数を 2 倍した値と 2^n (n は x のビット数) との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少なくとも 1 つの評価手段を具備することを特徴とする関数のランダム性評価装置。

【請求項 2】 請求項 1 記載の関数のランダム性評価装置において、

評価すべき関数 $S(x)$ について、予め決められた Δx , Δy に対し $S(x) + S(x + \Delta x) = \Delta y$ を満す x の数を求めて差分解読法に対する耐性を評価する差分解読法耐性評価手段と、

評価すべき関数についてその入力 x とそのマスク値 Γx の内積が、関数出力値 $S(x)$ とそのマスク値 Γy との内積が等しくなる x の数を 2 倍した値と、 2^n との差を求めて、線形解読法に対する耐性と評価する線形解読法耐性評価手段との少なくとも 1 つを備えることを特徴とする関数のランダム性評価装置。

【請求項 3】 代数構造の異なる複数の関数を組合わせた複数のパラメータ

を有する候補関数群を生成する候補関数生成手段と、

上記各候補関数群のそれぞれについて、解読攻撃に対する耐性を評価する耐性評価手段と、

上記耐性評価された候補関数群の耐性の強いものを選出する選択手段と、
を具備するランダム関数生成装置。

【請求項4】 請求項3記載のランダム関数生成装置において、

上記代数構造の異なる関数の1つは差分解読法及び線形解読法に対する各耐性が強いものであることを特徴とするランダム関数生成装置。

【請求項5】 請求項3又は4記載のランダム関数生成装置において、

上記耐性評価手段は、上記候補関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価手段と、

上記候補関数に対し、鍵 k を固定して x を入力して、素数 p 又は p のべき乗個の要素からなるガロア体上の多項式を用いて出力 $y = f_k(x)$ を表現して、上記多項式の項数を求めて、補間攻撃法に対する耐性を評価する補間攻撃耐性評価手段と、

上記候補関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関係のその平均的対応関係に対する偏よりを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と

上記候補関数 $S(x)$ について予め決められた Δx に対し $(S(x) + S(x + \Delta x))$ と出力のマスク値 Γy との内積が1である x の数を2倍した値と 2^n (n は x のビット数)との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少なくとも1つよりなることを特徴とするランダム関数生成装置。

【請求項6】 代数構造の異なる複数の関数を組合わせた複数のパラメータ

を有する候補関数群を生成する候補関数生成処理と、

上記各候補関数について、各パラメータに各種値を設定し、各種入力値に対する出力値をそれぞれ演算する演算処理と、

上記演算処理の結果を記憶手段に記憶する処理と、

上記記憶手段に記憶された値を用いて上記各候補関数のそれぞれについて、解読攻撃に対する耐性を評価する耐性評価処理と、

その耐性評価処理結果にもとづき、耐性の強い候補関数を選択出力する選択処理と、

をコンピュータにより実行させるプログラムを記録した記録媒体。

【請求項 7】 請求項 6 記載の記録媒体において、

上記耐性評価処理は、

上記候補関数により決まるブール関数の次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し他を除去する処理と、

その残された候補関数 $S(x)$ について、予め決められた Δx , Δy に対し $S(x) + S(x + \Delta x) = \Delta y$ を満す x の数を求めて差分解読法に対する耐性を評価する差分解読法耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数についてその入力 x とそのマスク値 Γx の内積が、関数出力値 $S(x)$ とそのマスク値 Γy との内積が等しくなる x の数を 2 倍した値と 2^n との差を求めて、線形解読法に対する耐性を評価する線形解読法耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残りの候補関数 $S(x)$ について予め決められた Δx に対し $(S(x) + S(x + \Delta x))$ と出力のマスク値 Γy との内積が 1 である x の数を 2 倍した値と 2^n (n は x のビット数) との差を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数の入力と出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の対応関数のその平均的対応関係に対する偏よりを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残し、他を除去する処理と、

その残された候補関数に対し、鍵 k を固定して x を入力して、素数 p 又は p のべき乗個の要素からなるガロア体上の多項式を用いて出力 $y = f_k(x)$ を表現して、上記多項式の項数を補間攻撃法に対する耐性を評価する補間攻撃耐性評価処理と、

その耐性評価が予め決めた値以上の候補関数を残して他を除去する処理とからなることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えば暗号装置等へ適用され、入力に対する出力が不規則に生成され、その動作を解析することが困難であるような関数を得るために、いくつかのランダム性指標を満たすかどうかを評価する装置、ランダム性指標を満たすと評価されたランダム関数を生成する装置およびそのプログラム記録媒体に関する。

【0002】

【従来の技術】

データを秘匿するためには暗号化技術が有効である。暗号化の方法は秘密鍵暗号方式と公開鍵暗号方式がある。一般に公開鍵暗号技術の方が安全性の証明技術の研究が進んでいるので、安全性の限界を知りつつ利用することができる。しかし、秘密鍵暗号については安全性の証明技術は確立されておらず、暗号攻撃が発見されると、その都度、個別に対処する必要が生じる。

【0003】

高速かつ安全な秘密鍵暗号を構成するために、暗号化対象のデータを適当な長さのブロックに分割し、そのブロック毎に暗号化する方法をブロック暗号と呼ぶ。通常ブロック暗号は暗号学的にあまり強くない関数を、平文に対し複数回繰り

返し適用することにより安全性を高めている。この、あまり強くない関数をF関数と呼ぶ。

【0004】

F関数の構成要素として、S-boxと呼ばれる、入力に対する出力が不規則

に生成され、その動作を解析することが困難であるような関数を用いることが一般的となっている。従来は、S-boxを構成する際に、安全性の根拠として、例えば、暗号化したデータの各ビットの0, 1の出現確率が統計的に1/2となる程度のことしか考えられておらず、ブロック暗号の理論的な安全性の根拠として不十分であった。

【0005】

実際、上記の基準を満たすブロック暗号に対する攻撃法として、差分解読法が文献「E.Biham, A.Shamir: "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol.4, No. 1, pp. 3-72」で、線形解読法が文献「M.Matsui: "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science 765), pp.386-397, Springer-Verlag, 1994」で提案され、多くのブロック暗号がこれらの解読法により解読できることがわかり、安全性の基準の見直しが必要となった。

【0006】

差分解読法や線形解読法が提案されてからブロック暗号にはこれらの解読法に対して強いことが要求されるようになった。そこで、これらの解読法に対して耐性があることを示す指標として、それぞれ最大平均差分確率や最大平均線形確率が文献「松井 充:『ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について』第18回情報理論とその応用シンポジウム予稿集(C-2-5), pp. 175-178」(以下「SITA 95-C-2-5」と略す)で提案された。これらの指標は小さいほどそれぞれの解読法に対する耐性があることが示されている。

【0007】

さらに近年、差分解読法や線形解読法に対する耐性のある暗号でも、これ以外の解読法によって解読されることが指摘され、さらに安全性の基準の見直しが必要となった。具体的には、文献「T.Jakobsen, L.R.Knudsen: "The Interpolation Attack on Block Cipher," Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267), pp.28-40, Springer Verlag,1997」(以下文献Aと記す)において、差分解読法や線形解読法に対する耐性のある

暗号でも、高階差分攻撃や補間攻撃によって解読される暗号があることが示された。

【0008】

さらに高階差分攻撃や補間攻撃以外にも文献「C.Harpes, J.L.Massey: "Partitioning Cryptanalysis, " Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267), pp.13-27, Springer Verlag, 1997」において線形解読法を一般化した分割攻撃が提案され、この攻撃に対しても十分な耐性があることを保証することが必要となっている。

【0009】

【発明が解決しようとする課題】

差分解読法、線形解読法に対する安全性を保証する技術が、一部のブロック暗号の構成法に対して確立しているのに対して、高階差分攻撃、補間攻撃、分割攻撃に対して完全に耐性があることを保証する技術は現時点では確立していない。すなわち、暗号がこれらの攻撃に対して安全であるためにランダム関数、いわゆる S-b-o-x が満たすべき必要十分条件は明らかになっていない。

【0010】

しかし、S-b-o-x を設計する上で、これらの攻撃法に対しても十分な強度をもつようにすることは重要な課題である。

そこで、この発明の一目的は、上記の各攻撃法に対し、その攻撃法に対する強度と深く関わる指標を見出し、その指標が（各攻撃に対して強いことを保証する必要十分条件を満たさないまでも、）各攻撃に対して耐性をもつための必要条件を示し、それらの一部または全ての条件を満たすような S-b-o-x 評価装置を提供することにある。

【0011】

さらに、この発明の他の目的はこれらの強度指標を満たす S-b-o-x の構成装置とそのプログラム記録媒体を提供することにある。

【0012】

【課題を解決するための手段】

第1発明によれば、高階差分攻撃法、補間攻撃法、分割攻撃法、に対する強度

指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を設定し、候補となる関数群について上記の一部または全ての条件が満たされるかどうかを評価し、必要に応じて上記の一部または全ての条件が満たされるものを選ぶ。更に、この選ばれたものは差分解読法、線形解読法の少くとも一方に対して耐性が強いことが評価される。

【0013】

以下に差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法に対する強度指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を述べる。以下では n 、 m を任意の自然数とし、 $S = \text{box}$ (ランダム関数) として n ビット入力、 m ビット出力の関数 $S : GF(2)^n \rightarrow GF(2)^m$ を考える。 $GF(2)^n$ は全ての n ビットデータの集合を示す。

【0014】

差分解読法に対する耐性をもつための必要条件

$S = \text{box}$ の差分解読法に対する耐性を示す指標として差分攻撃指標を定義し、その測定方法を述べ、差分解読法に対する耐性をもつための必要条件を示す。

差分解読法では、 $S = \text{box}$ の2つの入力の差分(入力差分値)に対する出力の差分(出力差分値)を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

【0015】

$S = \text{box}$ の入力を x 、入力差分値を Δx 、出力差分値を Δy とすると、ある入力差分値 Δx と、出力差分値 Δy に対して、全ての n ビット入力 x のうち、式(1)を満たす x の個数を $\delta_s(\Delta x, \Delta y)$ とする。但し、通常、“+”はビット毎の排他的論理和(XOR)で定義される。文献「X.Lai, J.L.Massey, and S.Murphy. "Markov Ciphers and Differential Cryptanalysis." In D.W.Davies, editor, *Advances in Cryptology-EUROCRYPT '91*, Volume 547 of Lecture Notes

in Computer Science, pp. 17-38. Springer-Verlag, Berlin, Heidelberg, New York, 1991」で述べられているように、一般的な逆元がある二項演算を用いて定義できる。

【0016】

$$S(x) + S(x + \Delta x) = \Delta y \quad (1)$$

これを書き換えると、 $\delta_s(\Delta x, \Delta y)$ は式(2)のように書ける。但し、 $\# \{x \mid \text{条件式}\}$ は条件式を満たす x の個数とする。

$$\delta_s(\Delta x, \Delta y) = \# \{x \in GF(2)^n \mid (S(x) + S(x + \Delta x)) = \Delta y\} \quad (2)$$

入力差分値として0を除く全ての n ビットデータ Δx と出力差分値として全ての m ビットデータ Δy に対して、式(2)より $\delta_s(\Delta x, \Delta y)$ を計算することができる。このうち最も大きい値をとる Δx と Δy の組合せが差分解読法における脆弱点となるため、 $\delta_s(\Delta x, \Delta y)$ の最大値が小さいほど差分解読法に対する耐性が高いということになる。よって式(3)で示される差分解読指標 Δ_s が小さいことが差分解読法に対して耐性をもつための必要条件となる。

【0017】

$$\Delta_s = \max \delta_s(\Delta x, \Delta y) \quad (3)$$

\max は $\Delta x \neq 0$ 、 Δy の全組合せの中から最大値を選ぶという条件とする
線形解読法に対する耐性をもつための必要条件

S-box の線形解読法に対する耐性を示す指標として線形攻撃指標を定義し、その測定方法を述べ、線形解読法に対する耐性をもつための必要条件を示す。

【0018】

線形解読法では、S-box の入力値と出力値のビット単位での任意の線形和(排他的論理和)を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

S-box の入力を x 、入力マスク値を Γx 、出力マスク値を Γy とすると、ある入力マスク値 Γx と出力マスク値 Γy に対して、式(4)で定義される $\lambda_s(\Gamma x, \Gamma y)$ が計算できる。但し、通常、“ \cdot ” は内積で定義される。 $x \cdot \Gamma x$ の意味は、マスク値 Γx 中の“0”に対応する x 中のビット値は無視し、“1”に対応する x 中のビット値のみを有効として、それらの和をとることを表わす

。すなわち、 $x \cdot \Gamma x = \sum x_i$ (\sum は Γx 中の第 i ビットが“1”の総和) 但し $x = (x_{n-1}, \dots, x_0)$ とする。

【0019】

$$\lambda_s(\Gamma x, \Gamma y)$$

$$= | 2 \times \# \{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n | \quad (4)$$

入力マスク値として全ての n ビットデータ Γx と、出力マスク値として0を除く全ての m ビットデータ Γy に対して、式(4)より $\lambda_s(\Gamma x, \Gamma y)$ を計算することができる。このうち最も大きい値をとる Γx と Γy の組合せが線形解読法における脆弱点となるため、 $\lambda_s(\Gamma x, \Gamma y)$ の最大値が小さいほど線形解読法に対する耐性が大きいということになる。よって式(5)で示される線形解読指標 Λ_s が小さいことが線形解読法に対して耐性をもつための必要条件となる。

【0020】

$$\Lambda_s = \max \lambda_s(\Gamma x, \Gamma y) \quad (5)$$

\max は $\Gamma x, \Gamma y \neq 0$ の全ての組合わせの中から最大値を選ぶという条件とする

高階差分攻撃法に対する耐性をもつための必要条件

S-boxの高階差分攻撃法に対する耐性を示す指標として高階差分攻撃指標を定義し、その測定方法を述べ、高階差分攻撃法に対する耐性をもつための必要条件を示す。

【0021】

高階差分攻撃法とは、暗号化途中の中間出力を入力に関して高階差分をとると、鍵によらない定数になることを利用した攻撃法である。暗号化途中の任意の中間データの任意のビットは、入力に関するブール多項式で表現できる。そのブール多項式の次数が d であった時、 $d+1$ 階差分をとると、その結果は鍵によらない定数になることから、これまでに、ブール多項式の次数が低い暗号に対する攻撃が前記文献Aで報告されている。

【0022】

F関数のブール多項式表現の次数が低ければ、F関数の繰り返し回数が十分多くないと暗号全体のブール多項式表現の次数も高くなり、解読される危険性が高い。よって、F関数の構成要素であるS-boxのブール多項式表現の次数も高いことが、F関数の繰り返し回数を増やすことなくその暗号が高階差分攻撃に対して安全にするための必要条件といえる。

【0023】

$S - box S : GF(2)^n \rightarrow GF(2)^m ; x \rightarrow S(x)$ に対し、

$$y = S(x),$$

$$x = (x_{n-1}, x_{n-2}, \dots, x_0) \in GF(2)^n,$$

$$y = (y_{m-1}, y_{m-2}, \dots, y_0) \in GF(2)^m$$

とする。また、変数集合 $X = \{x_{n-1}, x_{n-2}, \dots, x_0\}$ を定義する。この時、 $y_i = S_i(x)$ なるブール関数 $S_i : GF(2)^n \rightarrow GF(2) ; x \rightarrow S_i(x)$ を定義し、変数集合 X に関するブール関数 $S_i (0 \leq i \leq m-1)$ の次数を $\deg_x S_i$ とする。以下のように $\deg_x S_i (0 \leq i \leq m-1)$ の最小値を $\deg_x S$ とし、これが高階差分攻撃指標となる。

【0024】

$$\deg_x S = \min (\deg_x S_i) \quad (6)$$

\min は $0 \leq i \leq m-1$ を条件とする

高階差分攻撃に対して安全であるために $S - box$ が満たすべき必要条件は、 $\deg_x S$ が大きい値をもつことである。 S が全単射であれば、 $\deg_x S$ の最大値は $n-1$ であることが知られている。

補間攻撃法に対する耐性をもつための必要条件

$S - box$ の補間攻撃法に対する耐性を示す指標として補間攻撃指標を定義し、その測定方法を述べ、補間攻撃法に対する耐性をもつための必要条件を示す。

【0025】

補間攻撃の原理は次の通りである。鍵 k を固定した時、暗号文 y は、平文 x についての $GF(q)$ 上多項式 $f_k(x)$ を用いて $y = f_k(x)$ と表すことができる。但し、 q は素数または素数のべき乗である。 $f_k(x)$ に含まれる x についての項数が c である時、異なる c 組の平文とそれに対する暗号文の組 $(x_i, y_i) (1 \leq i \leq c)$ が与えられれば、ラグランジェ補間公式などにより、 $f_k(x)$ を構成することができる。これにより、任意の平文 x に対する暗号文を得ることができる。

【0026】

$f_k(x)$ に含まれる項数が多いほど、 $GF(q)$ 上多項式表現 $f_k(x)$ を用いた補間攻撃に必要な平文と暗号文の組は多くなり、攻撃は困難または不可能

となる。

$S - box$ の $GF(q)$ 上多項式表現に含まれる項数が少ないと、暗号全体の $GF(q)$ 上多項式表現に含まれる項数が少なくなる可能性がある。もちろん、 $S - box$ の $GF(q)$ 上多項式表現に含まれる項数が多くても、暗号全体を構成する上で項が打ち消し合い、暗号全体の $GF(q)$ 上多項式表現に含まれる項数が少なくならないよう注意する必要があるが、これは暗号構成法に関することであり、 $S - box$ の補間攻撃指標としては $GF(q)$ 上多項式表現に含まれる項数が多いことが補間攻撃法に対する耐性をもつための必要条件となる。 $S - box$ の関数 S の $GF(q)$ 上多項式表現に含まれる項数を $\text{coeff}_q S$ とし、これを $GF(q)$ 上多項式表現を利用する補間攻撃の攻撃指標とする。

【0027】

補間攻撃は想定される q として取りうる場合の数だけ攻撃が存在するので、なるべく多くの $GF(q)$ 上多項式表現に対してその項数 $\text{coeff}_q S$ を計算し、それらが小さい値をとらないことを確認する必要がある。

分割攻撃法に対する耐性をもつための必要条件

$S - box$ の分割攻撃法に対する耐性を示す指標として分割攻撃指標を定義し、その測定方法を述べ、分割攻撃法に対する耐性をもつための必要条件を示す。

【0028】

分割攻撃法では、平文集合全体のある部分集合と暗号文集合全体のある部分集合に成り立つ何らかの指標を観測し、大きな偏りが見い出される場合に、これを利用して暗号全体の解読につなげることができる。この「何らかの指標 I 」としては、文献「C.Harpes, J.L.Massey: "Partitioning Cryptanalysis," Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267), pp.13-27, Springer Verlag, 1997」では peak imbalance と squared Euclidean imbalance が例として挙げられている。

【0029】

文献「浜出 猛, 横山尚史, 島田 徹, 金子敏信: 『DES暗号に対する partitioning cryptanalysis of DES』, 1998年暗号と情報セキュリティシンポジウム予稿集(SCIS'98-2.2.A)」において、 $S - box$ の入出力集合に対して観

測される偏りを利用して、暗号全体の攻撃に成功していることから、S-boxの入出力集合に対して同様に定義された分割攻撃指標が暗号全体が分割攻撃法に対する耐性をもつための必要条件であることが分かる。

【0030】

S-boxの全入力集合を q 分割し、各部分集合を F_0, F_1, \dots, F_{q-1} 、全出力集合を m 分割し、各部分集合を G_0, G_1, \dots, G_{m-1} とする。各部分集合に含まれる要素数は全て等しいとする。入力 x を各部分集合の添字 $\{0, 1, \dots, q-1\}$ に写像する関数 f を入力分割関数、出力 y を $\{0, 1, \dots, m-1\}$ に写像する関数 g を出力分割関数と呼ぶ、つまり x がどの部分集合に属するかを示す関数が f であり、 y がどの部分集合に属するかを決める関数が g である。分割 F, G をそれぞれ

$$F = \{F_0, F_1, \dots, F_{q-1}\},$$

$$G = \{G_0, G_1, \dots, G_{m-1}\}$$

とすると、S-boxの分割対 (F, G) の偏り $I_S((F, G))$ は式(7)で与えられる。

【0031】

$$I_S((F, G)) = (1/q) \sum_{i=0}^{q-1} I(g(S(x)) | f(x) = i) \quad (7)$$

これがS-boxの分割攻撃指標であり、 $0 \sim 1$ の何れかの値を取り、その値と $1/2$ との差が小さいことが分割攻撃法に対する耐性をもつための必要条件となる。

次に、第2発明について述べる。文献「T.Jakobsen, L.R.Knudsen: "The Interpolation Attack on Block Cipher," Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267), pp.28-40, Springer Verlag, 1997」で挙げられている例により、差分解読法や線形解読法に対する耐性をもつ関数として、ある代数構造をもつ関数を選んでS-boxとして採用し、その代数構造を壊さない演算のみと組み合わせて暗号全体を構成すると、高階差分攻撃法や補間攻撃法などの代数攻撃法により容易に解読されることが分かっている。よって、第2発明の実施例は差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた（例えば

、関数の合成など) 関数を候補の関数群として選び、その関数群のそれぞれについてその解読に対する耐性を評価し、耐性の強いものを選択する。

【0032】

なお、この発明における候補関数群の選び方は必ずしも以上の手段に限定される必要はない。

作用

従来は、S-box設計(ランダム性評価)の指針として、例えば、暗号化したデータの各ビットの0, 1の出現確率が統計的に $1/2$ となる程度のことしか考えられておらず、暗号全体の攻撃に直結する評価指標が用いられることは少なかったが第1発明によれば、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、その他想定される攻撃法に対する耐性をもつかどうか評価する装置を加えることで、上記の暗号攻撃に対する高い安全性をもつ暗号を設計できることが期待される。

【0033】

このようにして攻撃に対する耐性が評価されたが、耐性の強いランダム関数を生成するには、候補となる関数群をどのように選ぶかという問題点が生じる。膨大な関数の中から上記の条件を満たす関数を選ぶのには多くの計算量を必要とするためである。

これを、第2発明の実施例によれば差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた(例えば、関数の合成など)関数を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

【0034】

【発明の実施の形態】

図1にこの発明によるランダム関数生成装置、関数のランダム性評価装置の実施例の機能構成を示す。入力手段1により生成しようとする関数のもととなるもの、そのパラメータなどが入力され、候補関数生成手段2において、入力手段1

の入力に応じた候補関数が生成され、そのパラメータ値と入力値とこれらにもとづく演算結果（出力値）とが記憶部 3 に記憶される。記憶部 3 に記憶された各種データが読出され、差分解読法耐性評価手段 4、線形解読法耐性評価手段 5、高階差分攻撃法耐性評価手段 6、補間攻撃法耐性評価手段 7、分割攻撃法耐性評価手段 8、その他の指標評価手段 9 でそれぞれ耐性評価、指標評価などがなされる。その各結果にもとづき、耐性の強い候補関数が関数選択手段 10 で選択され、記憶部 11 に記憶され、所要のものが出力手段 12 から出力される。

【0035】

この発明による関数がランダム性評価装置においては、入力手段 1 から評価されるべき関数が、各手段 4～9 に入力されて、ランダム性評価が行われる。

この実施例では、特願平 10-013572 データ変換装置中の S-box として用いる 8 ビット入出力の S-box の設計法について述べる。

まず、S-box の候補関数として、例えば図 2 に示すように関数 $P(x, e)$ を生成する手段 21 と、 $P(x, c)$ と代数構造を異にする関数 $A(y, a, b)$ を生成する手段 22 とが合成されたものとする。

【0036】

$S: GF(2)^8 \rightarrow GF(2)^8; x \rightarrow A((P(x, e)), a, b),$
但し

$$P(x, e) = x^e \text{ in } GF(2^8) \quad (8)$$

$$A(y, a, b) = ay + b \pmod{2^8} \quad (9)$$

である。 $P(x, e)$ はガロア体 $GF(2^8)$ 上で定義されるべき乗関数である。この時、パラメータ a, b, e は 0 以上 255 以下の任意の自然数という自由度がある。このうち、パラメータ a, b のハミング重みを 3 以上 5 以下に限定し、つまり a, b は各 8 ビットであるがそのうち“1”（又は“0”）が 3 ビット以上 5 ビット以下であり、さらに S-box が全単射であること、差分解読法、

線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法に対する耐性があるための必要条件を満たすかどうかを評価し、パラメータ a, b, e を絞り込んでいく。

。

【0037】

その例、つまりこの発明の装置の一実施例の処理手順を図3に示す。なお、実施例はこの例に限られない。S-boxの候補とする関数の選び方には自由度がある。またS-boxの設計指標も数多くあり、その優先順位や候補関数の絞り込みの順序など、多くの自由度がある。

図3において、ステップS1で候補関数Sが全単射であるかを評価する。パラメータaが奇数、eが $2^8 - 1 = 255$ と互いに素である時、関数Sは全単射になるので、これらを満たすパラメータを選択し、満たさないものは候補から除く。この処理は図1中の手段9により行う。あるいはパラメータaは入力手段1で奇数のみを入力することで得る。

【0038】

eのハミング重みと式(6)で表わせる高階差分攻撃指標 $\deg_x S$ とが等しいことが知られている。そこでステップS2で、残りの候補関数Sの高階差分攻撃指標 $\deg_x S$ の条件を満たすため、ここでは $\deg_x S$ の最大値、つまりeのハミング重みが7になるものを選択する。これを満たさないものは候補から除く。

ステップS3で残りの関数Sの差分攻撃指標 Δ_S の条件を満たすため、関数Sの差分攻撃指標 Δ_S が最小となるものを選択する。これを満たさないものは候補から除く。

【0039】

ステップS4で残りの候補関数Sの線形攻撃指標 Λ_S の条件を満たすため、関数Sの線形攻撃指標 Λ_S が最小となるものを選択する。これを満たさないものは候補から除く。

ステップS5では以下の式で定義される関数Sの差分線形攻撃指標 Ξ_S が最小となるものを選択する。これを満たさないものは候補から除く。

【0040】

$$\xi_S(\Delta x, \Gamma y) = |2 \times \# \{x \in GF(2)^8 \mid (S(x) + S(x + \Delta x)) \cdot \Gamma y = 1\} - 2^8|$$

$$\Xi_S = \max \xi_S(\Delta x, \Gamma y)$$

maxは $\Delta x \neq 0, \Gamma y \neq 0$ の全組み合わせの中から最大値を選ぶという条件とする

k を n 以下の自然数とした時、

【0041】

【数1】

$S : GF(2)^n \rightarrow GF(2)^n : x \rightarrow x^{2^k} \text{ in } GF(2^n)$ 、

または $S : GF(2)^n \rightarrow GF(2)^n : x \rightarrow x^{2^{k+1}} \text{ in } GF(2^n)$ の時、

この指標が最大値 2^n をとることが示される。これが直接何らかの攻撃に結びつく例はまだ報告されていないが、この指標についてもなるべく小さい値をとる（顕著な偏りが無い）ことが望ましいため、パラメータの選択基準に加えた。

この結果、以下のパラメータまで絞り込める。

【0042】

$(a, b) = (97, 97), (97, 225), (225, 97), (225, 225)$

$e = 127, 191, 223, 239, 247, 251, 253, 254$

次に、ステップ S 6 で残りの候補、関数 S の分割攻撃指標 $I_S((F, G))$ の条件を満たすため、上記のパラメータの全ての組み合わせのうち、関数 S の分割攻撃指標 $I_S((F, G))$ が $1/2$ に近いかどうかを確認する。 $1/2$ との差が大きいものがあれば候補から除く。

【0043】

ステップ S 7 で更に残りの候補関数 S の $GF(2^8)$ 上の多項式を利用する補間攻撃指標 $\text{coeff}_q S$ (ただし $q = 2^8$) の条件を満たすため、上記パラメータの全ての組み合わせのうち、関数 S の $GF(2^8)$ 上の多項式を利用する補間攻撃指標 $\text{coeff}_q S$ が大きいかどうかを確認する。小さいものがあれば候補から除く。

【0044】

ステップ S 8 では、 $2^8 + 1$ 以上 2^9 以下の全ての素数 p について、関数 S の $GF(p)$ 上の多項式を利用する補間攻撃指標 $\text{coeff}_p S$ の条件を満たすため、関数 S の $GF(p)$ 上の多項式を利用する補間攻撃指標 $\text{coeff}_p S$ が大きいかどうか、この例では最大値をとるかどうかを確認する。小さいものがあれば候補から除く。

【0045】

以上の評価の結果、以下のパラメータの組み合わせ（全32種類）が残る。

$$(a, b) = (97, 97), (97, 225), (225, 97), (225, 225)$$

$$e = 127, 191, 223, 239, 247, 251, 253, 254$$

この結果はステップS5での結果と同一である。つまりこの例ではステップS5で既に本実施例で考慮するあらゆる攻撃法に対しても強い関数が得られたことになる。

【0046】

このようにして選択された32個の関数は上記の評価基準における強度は等しいので、S-boxとしてどの関数を選んでもよい。

S-boxの評価として、又は関数生成において、解読計算量が現実的に計算可能な値から各種の攻撃に対する各評価指標の基準が決定され、これらの基準を全て越えれば、そのランダム性は合格、あるいはその関数は使用してもよいと、その要求されるランダム性の程度、つまり各種の攻撃に対する強さに応じて各指標に対するしきい値（基準値）が決定される。

【0047】

【発明の効果】

以上述べたように、この発明によれば、暗号装置等の構成要素となるS-box関数のランダム性評価方法およびその装置において、従来の評価方法に加えて、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、その他想定される攻撃法に対する耐性をもつかどうか評価する手段を加えることで、ランダム性の評価を正しく行え、かつ上記の暗号攻撃に対する高い安全性をもつ暗号が設計できる。

【0048】

さらに、候補となる関数群を差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた関数を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

【0049】

また図3に示したような手順で絞り込みを行うと、少ない演算量で効率的に絞り込みを行うことができる。

また、候補となる関数群をランダムに選ぶのではなく、よく知られた異なる代数構造をもつ関数の組み合わせから選ぶことで、S-boxにトラップドア（設計者だけがその暗号を解読できるような秘密のしかけ）がないことも示しやすい。

【図面の簡単な説明】

【図1】

この発明によるランダム関数生成装置、関数のランダム性評価装置の機能的構成例を示すブロック図。

【図2】

この発明によるランダム関数生成装置の基本構成の例を示すブロック図。

【図3】

この発明によるランダム関数生成装置の実施例の処理手順の例を示す流れ図。

【書類名】 図面

【図 1】

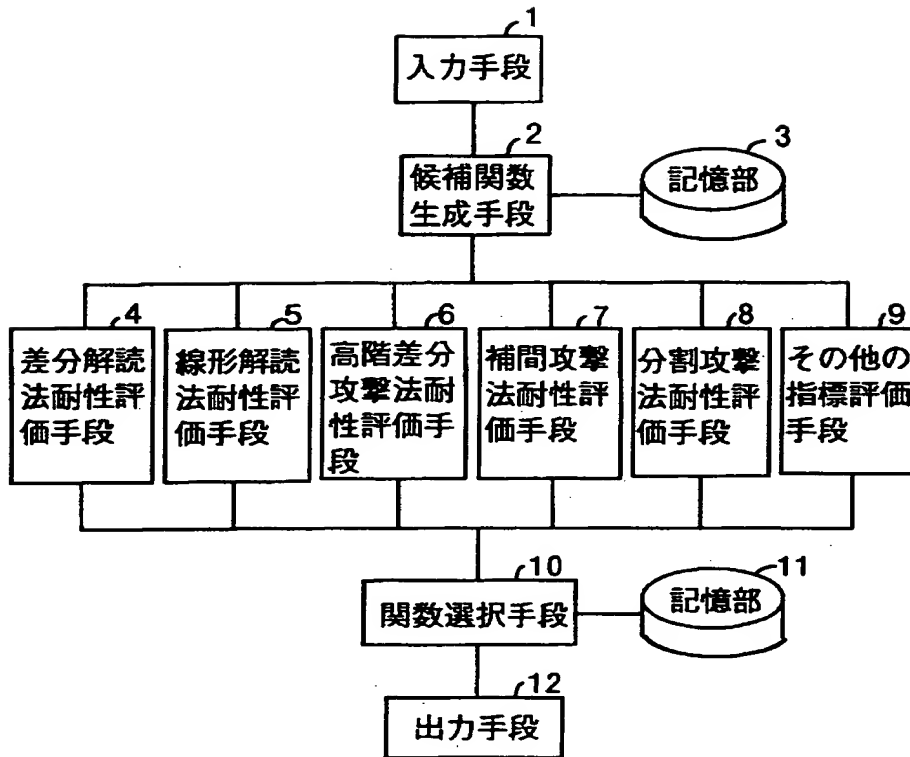


図 1

【図 2】

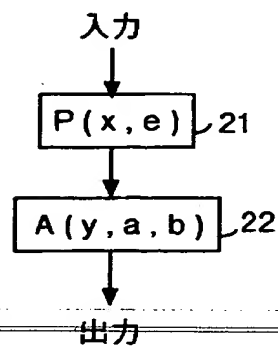
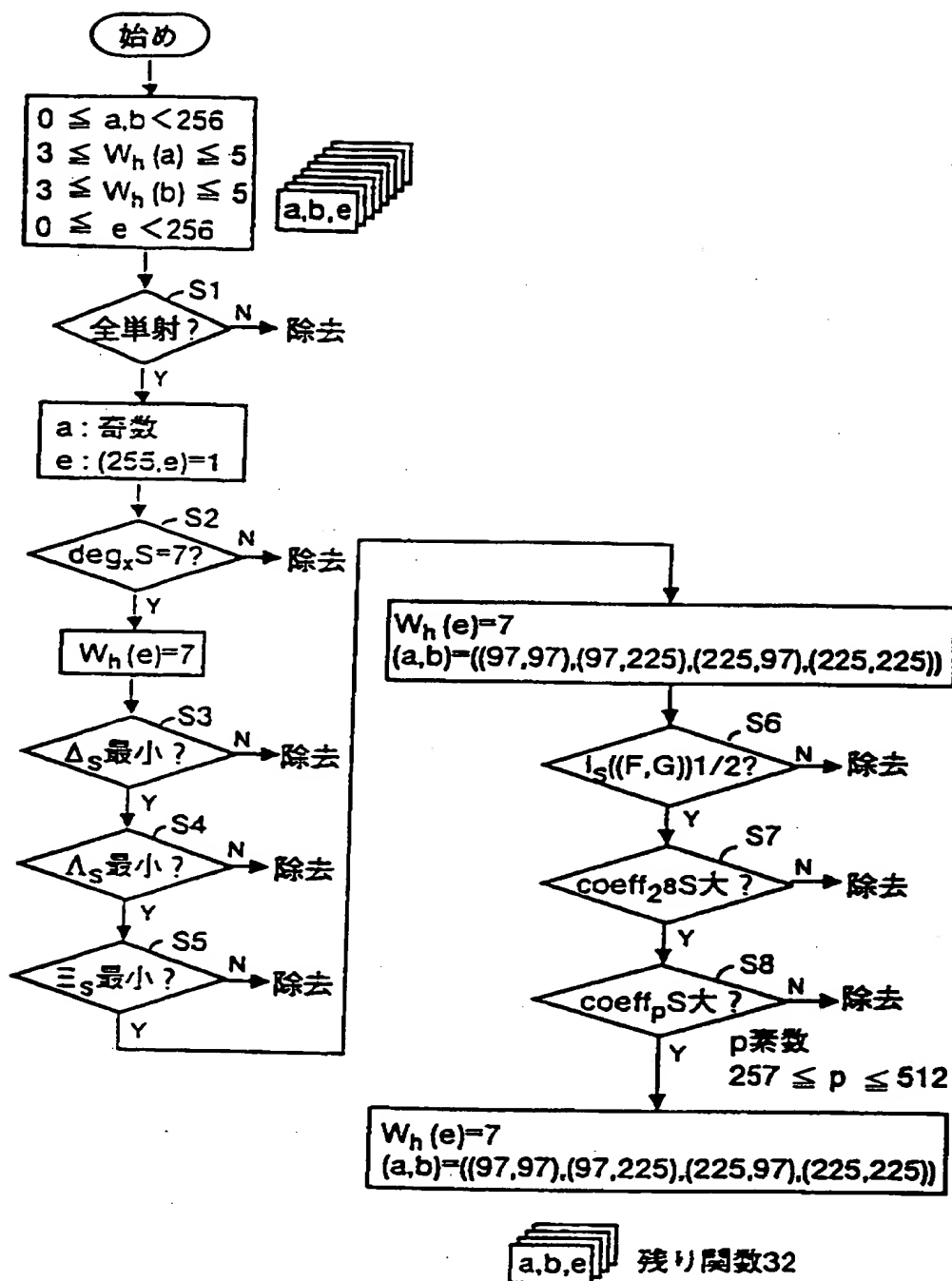


図 2

【図3】



— 図 3 —

【書類名】 要約書

【要約】

【課題】 差分解読法、線形解読法のみならず、高階差分攻撃法、補間攻撃法、分割攻撃法に対しても耐性が強い暗号化関数を生成する。

【解決手段】 $S = A((P(x, e)), a, b)$ 、 $P(x, e) = x^e \text{ in } GF(2^8)$ 、 $A(y, a, b) = ay + b \pmod{2^8}$ を候補とし a, b のハミング重みを3以上5以下とし、 a を奇数、 e を255と互いに素とし (S1)、他の候補を除き、 S のブール多項式の次数 $\deg_x S$ が最大のものを選び (S2)、差分攻撃指標 Δ_S が最小のもの、線形攻撃指標 Λ_S が最小のものを選び (S3, S4)、更に差分線形攻撃指標 Ξ_S が最小のものを選び (S5)、分割攻撃指標 $I_S((F, G))$ が $1/2$ に近いものを選び (S6)、補間攻撃指標が大きいものを選ぶ (S7, S8)。

【選択図】 図3

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000004226

【住所又は居所】 東京都新宿区西新宿三丁目19番2号

【氏名又は名称】 日本電信電話株式会社

【代理人】 申請人

【識別番号】 100066153

【住所又は居所】 東京都新宿区新宿四丁目2番21号 相模ビル

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【住所又は居所】 東京都新宿区新宿4丁目2番21号 相模ビル 草
野特許事務所

【氏名又は名称】 稲垣 稔

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日
[変更理由] 住所変更
住 所 東京都新宿区西新宿三丁目19番2号
氏 名 日本電信電話株式会社